

SY0-701 Dumps

CompTIA Security+ Exam

<https://www.certleader.com/SY0-701-dumps.html>



NEW QUESTION 1

Employees in the research and development business unit receive extensive training to ensure they understand how to best protect company data. Which of the following is the type of data these employees are most likely to use in day-to-day work activities?

- A. Encrypted
- B. Intellectual property
- C. Critical
- D. Data in transit

Answer: B

Explanation:

Intellectual property is a type of data that consists of ideas, inventions, designs, or other creative works that have commercial value and are protected by law. Employees in the research and development business unit are most likely to use intellectual property data in their day-to-day work activities, as they are involved in creating new products or services for the company. Intellectual property data needs to be protected from unauthorized use, disclosure, or theft, as it can give the company a competitive advantage in the market. Therefore, these employees receive extensive training to ensure they understand how to best protect this type of data. References = CompTIA Security+ SY0-701 Certification Study Guide, page 90; Professor Messer's CompTIA SY0-701 Security+ Training Course, video 1.2 - Security Concepts, 7:57 - 9:03.

NEW QUESTION 2

Which of the following is the best reason to complete an audit in a banking environment?

- A. Regulatory requirement
- B. Organizational change
- C. Self-assessment requirement
- D. Service-level requirement

Answer: A

Explanation:

A regulatory requirement is a mandate imposed by a government or an authority that must be followed by an organization or an individual. In a banking environment, audits are often required by regulators to ensure compliance with laws, standards, and policies related to security, privacy, and financial reporting. Audits help to identify and correct any gaps or weaknesses in the security posture and the internal controls of the organization. References:

- ? Official CompTIA Security+ Study Guide (SY0-701), page 507
- ? Security+ (Plus) Certification | CompTIA IT Certifications 2

NEW QUESTION 3

Which of the following must be considered when designing a high-availability network? (Choose two).

- A. Ease of recovery
- B. Ability to patch
- C. Physical isolation
- D. Responsiveness
- E. Attack surface
- F. Extensible authentication

Answer: AE

Explanation:

A high-availability network is a network that is designed to minimize downtime and ensure continuous operation even in the event of a failure or disruption. A high-availability network must consider the following factors:

? Ease of recovery: This refers to the ability of the network to restore normal functionality quickly and efficiently after a failure or disruption. Ease of recovery can be achieved by implementing backup and restore procedures, redundancy and failover mechanisms, fault tolerance and resilience, and disaster recovery plans.

? Attack surface: This refers to the amount of exposure and vulnerability of the network to potential threats and attacks. Attack surface can be reduced by implementing security controls such as firewalls, encryption, authentication, access control, segmentation, and hardening.

The other options are not directly related to high-availability network design:

? Ability to patch: This refers to the process of updating and fixing software components to address security issues, bugs, or performance improvements. Ability to patch is important for maintaining the security and functionality of the network, but it is not a specific factor for high-availability network design.

? Physical isolation: This refers to the separation of network components or devices from other networks or physical environments. Physical isolation can enhance the security and performance of the network, but it can also reduce the availability and accessibility of the network resources.

? Responsiveness: This refers to the speed and quality of the network's performance and service delivery. Responsiveness can be measured by metrics such as latency, throughput, jitter, and packet loss. Responsiveness is important for ensuring customer satisfaction and user experience, but it is not a specific factor for high-availability network design.

? Extensible authentication: This refers to the ability of the network to support multiple and flexible authentication methods and protocols. Extensible authentication can improve the security and convenience of the network, but it is not a specific factor for high-availability network design.

References = 1: CompTIA Security+ SY0-701 Certification Study Guide, page 972: High Availability – CompTIA Security+ SY0-701 – 3.4, video by Professor Messer.

NEW QUESTION 4

Which of the following methods to secure credit card data is best to use when a requirement is to see only the last four numbers on a credit card?

- A. Encryption
- B. Hashing
- C. Masking
- D. Tokenization

Answer: C

Explanation:

Masking is a method to secure credit card data that involves replacing some or all of the digits with symbols, such as asterisks, dashes, or Xs, while leaving some of the original digits visible. Masking is best to use when a requirement is to see only the last four numbers on a credit card, as it can prevent unauthorized access to the full card number, while still allowing identification and verification of the cardholder. Masking does not alter the original data, unlike encryption, hashing, or tokenization, which use algorithms to transform the data into different formats.

References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 2: Compliance and Operational Security, page 721. CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 2: Compliance and Operational Security, page 722.

NEW QUESTION 5

An engineer needs to find a solution that creates an added layer of security by preventing unauthorized access to internal company resources. Which of the following would be the best solution?

- A. RDP server
- B. Jump server
- C. Proxy server
- D. Hypervisor

Answer: B

Explanation:

= A jump server is a server that acts as an intermediary between a user and a target system. A jump server can provide an added layer of security by preventing unauthorized access to internal company resources. A user can connect to the jump server using a secure protocol, such as SSH, and then access the target system from the jump server. This way, the target system is isolated from the external network and only accessible through the jump server. A jump server can also enforce security policies, such as authentication, authorization, logging, and auditing, on the user's connection. A jump server is also known as a bastion host or a jump box. References = CompTIA Security+ Certification Exam Objectives, Domain 3.3: Given a scenario, implement secure network architecture concepts. CompTIA Security+ Study Guide (SY0-701), Chapter 3: Network Architecture and Design, page 101. Other Network Appliances – SY0-601 CompTIA Security+ : 3.3, Video 3:03. CompTIA Security+ Certification Exam SY0-701 Practice Test 1, Question 2.

NEW QUESTION 6

A data administrator is configuring authentication for a SaaS application and would like to reduce the number of credentials employees need to maintain. The company prefers to use domain credentials to access new SaaS applications. Which of the following methods would allow this functionality?

- A. SSO
- B. LEAP
- C. MFA
- D. PEAP

Answer: A

Explanation:

SSO stands for single sign-on, which is a method of authentication that allows users to access multiple applications or services with one set of credentials. SSO reduces the number of credentials employees need to maintain and simplifies the login process. SSO can also improve security by reducing the risk of password reuse, phishing, and credential theft. SSO can be implemented using various protocols, such as SAML, OAuth, OpenID Connect, and Kerberos, that enable the exchange of authentication information between different domains or systems. SSO is commonly used for accessing SaaS applications, such as Office 365, Google Workspace, Salesforce, and others, using domain credentials¹²³.

* B. LEAP stands for Lightweight Extensible Authentication Protocol, which is a Cisco proprietary protocol that provides authentication for wireless networks. LEAP is not related to SaaS applications or domain credentials⁴.

* C. MFA stands for multi-factor authentication, which is a method of authentication that requires users to provide two or more pieces of evidence to prove their identity. MFA can enhance security by adding an extra layer of protection beyond passwords, such as tokens, biometrics, or codes. MFA is not related to SaaS applications or domain credentials, but it can be used in conjunction with SSO.

* D. PEAP stands for Protected Extensible Authentication Protocol, which is a protocol that provides secure authentication for wireless networks. PEAP uses TLS to create an encrypted tunnel between the client and the server, and then uses another authentication method, such as MS-CHAPv2 or EAP-GTC, to verify the user's identity. PEAP is not related to SaaS applications or domain credentials.

References = 1: Security+ (SY0-701) Certification Study Guide | CompTIA IT Certifications 2: What is Single Sign-On (SSO)? - Definition from WhatIs.com 3: Single sign-on - Wikipedia 4: Lightweight Extensible Authentication Protocol - Wikipedia : What is Multi-Factor Authentication (MFA)? - Definition from WhatIs.com : Protected Extensible Authentication Protocol - Wikipedia

NEW QUESTION 7

Which of the following would be best suited for constantly changing environments?

- A. RTOS
- B. Containers
- C. Embedded systems
- D. SCADA

Answer: B

Explanation:

Containers are a method of virtualization that allows applications to run in isolated environments with their own dependencies, libraries, and configurations. Containers are best suited for constantly changing environments because they are lightweight, portable, scalable, and easy to deploy and update. Containers can also support microservices architectures, which enable faster and more frequent delivery of software features. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 10: Mobile Device Security, page 512 1

NEW QUESTION 8

A security analyst locates a potentially malicious video file on a server and needs to identify both the creation date and the file's creator. Which of the following actions would most likely give the security analyst the information required?

- A. Obtain the file's SHA-256 hash.
- B. Use hexdump on the file's contents.

- C. Check endpoint logs.
- D. Query the file's metadata.

Answer: D

Explanation:

Metadata is data that describes other data, such as its format, origin, creation date, author, and other attributes. Video files, like other types of files, can contain metadata that can provide useful information for forensic analysis. For example, metadata can reveal the camera model, location, date and time, and software used to create or edit the video file. To query the file's metadata, a security analyst can use various tools, such as MedialInfo1, ffprobe2, or hexdump3, to extract and display the metadata from the video file. By querying the file's metadata, the security analyst can most likely identify both the creation date and the file's creator, as well as other relevant information. Obtaining the file's SHA-256 hash, checking endpoint logs, or using hexdump on the file's contents are other possible actions, but they are not the most appropriate to answer the question. The file's SHA-256 hash is a cryptographic value that can be used to verify the integrity or uniqueness of the file, but it does not reveal any information about the file's creation date or creator. Checking endpoint logs can provide some clues about the file's origin or activity, but it may not be reliable or accurate, especially if the logs are tampered with or incomplete. Using hexdump on the file's contents can show the raw binary data of the file, but it may not be easy or feasible to interpret the metadata from the hex output, especially if the file is large or encrypted. References: 1: How do I get the meta-data of a video file? 2: How to check if an mp4 file contains malware? 3: [Hexdump - Wikipedia]

NEW QUESTION 9

Which of the following describes the process of concealing code or text inside a graphical image?

- A. Symmetric encryption
- B. Hashing
- C. Data masking
- D. Steganography

Answer: D

Explanation:

Steganography is the process of hiding information within another medium, such as an image, audio, video, or text file. The hidden information is not visible or noticeable to the casual observer, and can only be extracted by using a specific technique or key. Steganography can be used for various purposes, such as concealing secret messages, watermarking, or evading detection by antivirus software¹²

References:

1: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 5: Cryptography and PKI, page 233 2: CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 5: Cryptography and PKI, page 235

NEW QUESTION 10

Malware spread across a company's network after an employee visited a compromised industry blog. Which of the following best describes this type of attack?

- A. Impersonation
- B. Disinformation
- C. Watering-hole
- D. Smishing

Answer: C

Explanation:

A watering-hole attack is a type of cyberattack that targets groups of users by infecting websites that they commonly visit. The attackers exploit vulnerabilities to deliver a malicious payload to the organization's network. The attack aims to infect users' computers and gain access to a connected corporate network. The attackers target websites known to be popular among members of a particular organization or demographic. The attack differs from phishing and spear-phishing attacks, which typically attempt to steal data or install malware onto users' devices¹

In this scenario, the compromised industry blog is the watering hole that the attackers used to spread malware across the company's network. The attackers likely chose this blog because they knew that the employees of the company were interested in its content and visited it frequently. The attackers may have injected malicious code into the blog or redirected the visitors to a spoofed website that hosted the malware. The malware then infected the employees' computers and propagated to the network.

References¹: Watering Hole Attacks: Stages, Examples, Risk Factors & Defense ...

NEW QUESTION 10

Which of the following vulnerabilities is exploited when an attacker overwrites a register with a malicious address?

- A. VM escape
- B. SQL injection
- C. Buffer overflow
- D. Race condition

Answer: C

Explanation:

A buffer overflow is a vulnerability that occurs when an application writes more data to a memory buffer than it can hold, causing the excess data to overwrite adjacent memory locations. A register is a small storage area in the CPU that holds temporary data or instructions. An attacker can exploit a buffer overflow to overwrite a register with a malicious address that points to a shellcode, which is a piece of code that gives the attacker control over the system. By doing so, the attacker can bypass the normal execution flow of the application and execute arbitrary commands.

References: CompTIA Security+ SY0-701 Certification Study Guide, Chapter 2: Threats, Attacks, and Vulnerabilities, Section 2.3: Application Attacks, Page 76 1; Buffer Overflows - CompTIA Security+ SY0-701 - 2.3 2

NEW QUESTION 14

An analyst is evaluating the implementation of Zero Trust principles within the data plane. Which of the following would be most relevant for the analyst to evaluate?

- A. Secured zones
- B. Subject role
- C. Adaptive identity
- D. Threat scope reduction

Answer: D

Explanation:

The data plane, also known as the forwarding plane, is the part of the network that carries user traffic and data. It is responsible for moving packets from one device to another based on the routing and switching decisions made by the control plane. The data plane is a critical component of the Zero Trust architecture, as it is where most of the attacks and breaches occur. Therefore, implementing Zero Trust principles within the data plane can help to improve the security and resilience of the network.

One of the key principles of Zero Trust is to assume breach and minimize the blast radius and segment access. This means that the network should be divided into smaller and isolated segments or zones, each with its own security policies and controls. This way, if one segment is compromised, the attacker cannot easily move laterally to other segments and access more resources or data. This principle is also known as threat scope reduction, as it reduces the scope and impact of a potential threat.

The other options are not as relevant for the data plane as threat scope reduction. Secured zones are a concept related to the control plane, which is the part of the network that makes routing and switching decisions. Subject role is a concept related to the identity plane, which is the part of the network that authenticates and authorizes users and devices. Adaptive identity is a concept related to the policy plane, which is the part of the network that defines and enforces the security policies and rules.

References = <https://bing.com/search?q=Zero+Trust+data+plane> <https://learn.microsoft.com/en-us/security/zero-trust/deploy/data>

NEW QUESTION 15

An administrator notices that several users are logging in from suspicious IP addresses. After speaking with the users, the administrator determines that the employees were not logging in from those IP addresses and resets the affected users' passwords. Which of the following should the administrator implement to prevent this type of attack from succeeding in the future?

- A. Multifactor authentication
- B. Permissions assignment
- C. Access management
- D. Password complexity

Answer: A

Explanation:

The correct answer is A because multifactor authentication (MFA) is a method of verifying a user's identity by requiring more than one factor, such as something the user knows (e.g., password), something the user has (e.g., token), or something the user is (e.g., biometric). MFA can prevent unauthorized access even if the user's password is compromised, as the attacker would need to provide another factor to log in. The other options are incorrect because they do not address the root cause of the attack, which is weak authentication. Permissions assignment (B) is the process of granting or denying access to resources based on the user's role or identity. Access management (C) is the process of controlling who can access what and under what conditions. Password complexity (D) is the requirement of using strong passwords that are hard to guess or crack, but it does not prevent an attacker from using a stolen password. References = You can learn more about multifactor authentication and other security concepts in the following resources:

? CompTIA Security+ SY0-701 Certification Study Guide, Chapter 1: General Security Concepts¹

? Professor Messer's CompTIA SY0-701 Security+ Training Course, Section 1.2: Security Concepts²

? Multi-factor Authentication – SY0-601 CompTIA Security+ : 2.43

? TOTAL: CompTIA Security+ Cert (SY0-701) | Udemy, Section 3: Identity and Access Management, Lecture 15: Multifactor Authentication⁴

? CompTIA Security+ Certification SY0-601: The Total Course [Video], Chapter 3: Identity and Account Management, Section 2: Enabling Multifactor Authentication⁵

NEW QUESTION 20

Which of the following is a primary security concern for a company setting up a BYOD program?

- A. End of life
- B. Buffer overflow
- C. VM escape
- D. Jailbreaking

Answer: D

Explanation:

Jailbreaking is a primary security concern for a company setting up a BYOD (Bring Your Own Device) program. Jailbreaking is the process of removing the manufacturer's or the carrier's restrictions on a device, such as a smartphone or a tablet, to gain root access and install unauthorized or custom software. Jailbreaking can compromise the security of the device and the data stored on it, as well as expose it to malware, viruses, or hacking. Jailbreaking can also violate the warranty and the terms of service of the device, and make it incompatible with the company's security policies and standards. Therefore, a company setting up a BYOD program should prohibit jailbreaking and enforce device compliance and encryption. References = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 2, page 76. CompTIA Security+ SY0-701 Exam Objectives, Domain 2.4, page 11.

NEW QUESTION 25

A security analyst is reviewing the following logs:

```
[10:00:00 AM] Login rejected - username administrator - password Spring2023
[10:00:01 AM] Login rejected - username jsmith - password Spring2023
[10:00:01 AM] Login rejected - username guest - password Spring2023
[10:00:02 AM] Login rejected - username cpolk - password Spring2023
[10:00:03 AM] Login rejected - username fmartin - password Spring2023
```

Which of the following attacks is most likely occurring?

- A. Password spraying

- B. Account forgery
- C. Pass-the-hash
- D. Brute-force

Answer: A

Explanation:

Password spraying is a type of brute force attack that tries common passwords across several accounts to find a match. It is a mass trial-and-error approach that can bypass account lockout protocols. It can give hackers access to personal or business accounts and information. It is not a targeted attack, but a high-volume attack tactic that uses a dictionary or a list of popular or weak passwords¹².

The logs show that the attacker is using the same password ("password123") to attempt to log in to different accounts ("admin", "user1", "user2", etc.) on the same web server. This is a typical pattern of password spraying, as the attacker is hoping that at least one of the accounts has a weak password that matches the one they are trying. The attacker is also using a tool called Hydra, which is one of the most popular brute force tools, often used in cracking passwords for network authentication³.

Account forgery is not the correct answer, because it involves creating fake accounts or credentials to impersonate legitimate users or entities. There is no evidence of account forgery in the logs, as the attacker is not creating any new accounts or using forged credentials.

Pass-the-hash is not the correct answer, because it involves stealing a hashed user credential and using it to create a new authenticated session on the same network. Pass-the-hash does not require the attacker to know or crack the password, as they use the stored version of the password to initiate a new session⁴.

The logs show that the attacker is using plain text passwords, not hashes, to try to log in to the web server.

Brute-force is not the correct answer, because it is a broader term that encompasses different types of attacks that involve trying different variations of symbols or words until the correct password is found. Password spraying is a specific type of brute force attack that uses a single common password against multiple accounts⁵. The logs show that the attacker is using password spraying, not brute force in general, to try to gain access to the web server. References = 1:

Password spraying: An overview of password spraying attacks ... - Norton, 2: Security: Credential Stuffing vs. Password Spraying -

Baeldung, 3: Brute Force Attack: A definition + 6 types to know | Norton, 4: What is a Pass-the-Hash Attack? - CrowdStrike, 5: What is a Brute Force Attack? |

Definition, Types &

How It Works - Fortinet

NEW QUESTION 30

An administrator was notified that a user logged in remotely after hours and copied large amounts of data to a personal device. Which of the following best describes the user's activity?

- A. Penetration testing
- B. Phishing campaign
- C. External audit
- D. Insider threat

Answer: D

Explanation:

An insider threat is a security risk that originates from within the organization, such as an employee, contractor, or business partner, who has authorized access to the organization's data and systems. An insider threat can be malicious, such as stealing, leaking, or sabotaging sensitive data, or unintentional, such as falling victim to phishing or social engineering. An insider threat can cause significant damage to the organization's reputation, finances, operations, and legal compliance. The user's activity of logging in remotely after hours and copying large amounts of data to a personal device is an example of a malicious insider threat, as it violates the organization's security policies and compromises the confidentiality and integrity of the data. References = Insider Threats – CompTIA Security+ SY0-701: 3.2, video at 0:00; CompTIA Security+ SY0-701 Certification Study Guide, page 133.

NEW QUESTION 33

A company has begun labeling all laptops with asset inventory stickers and associating them with employee IDs. Which of the following security benefits do these actions provide? (Choose two.)

- A. If a security incident occurs on the device, the correct employee can be notified.
- B. The security team will be able to send user awareness training to the appropriate device.
- C. Users can be mapped to their devices when configuring software MFA tokens.
- D. User-based firewall policies can be correctly targeted to the appropriate laptops.
- E. When conducting penetration testing, the security team will be able to target the desired laptops.
- F. Company data can be accounted for when the employee leaves the organization.

Answer: AF

Explanation:

Labeling all laptops with asset inventory stickers and associating them with employee IDs can provide several security benefits for a company. Two of these benefits are:

? A. If a security incident occurs on the device, the correct employee can be notified.

An asset inventory sticker is a label that contains a unique identifier for a laptop, such as a serial number, a barcode, or a QR code. By associating this identifier with an employee ID, the security team can easily track and locate the owner of the laptop in case of a security incident, such as a malware infection, a data breach, or a theft. This way, the security team can notify the correct employee about the incident, and provide them with the necessary instructions or actions to take, such as changing passwords, scanning for viruses, or reporting the loss. This can help to contain the incident, minimize the damage, and prevent further escalation.

? F. Company data can be accounted for when the employee leaves the

organization. When an employee leaves the organization, the company needs to ensure that all the company data and assets are returned or deleted from the employee's laptop. By labeling the laptop with an asset inventory sticker and

associating it with an employee ID, the company can easily identify and verify the laptop that belongs to the departing employee, and perform the appropriate data backup, wipe, or transfer procedures. This can help to protect the company data from unauthorized access, disclosure, or misuse by the former employee or any other party.

The other options are not correct because they are not related to the security benefits of labeling laptops with asset inventory stickers and associating them with employee IDs. B. The security team will be able to send user awareness training to the appropriate device. User awareness training is a type of security education that aims to improve the knowledge and behavior of users regarding security threats and best practices. The security team can send user awareness training to the appropriate device by using the email address, username, or IP address of the device, not the asset inventory sticker or the employee ID.

* C. Users can be mapped to their devices when configuring software MFA tokens. Software MFA tokens are a type of multi-factor authentication that uses a software application to generate a one-time password or a push notification for verifying the identity of a user. Users can be mapped to their devices when configuring software MFA tokens by using the device ID, phone number, or email address of the device, not the asset inventory sticker or the employee ID. D. User-

based firewall policies can be correctly targeted to the appropriate laptops. User-based firewall policies are a type of firewall rules that apply to specific users or groups of users, regardless of the device or location they use to access the network. User-based firewall policies can be correctly targeted to the appropriate laptops by using the username, domain, or certificate of the user, not the asset inventory sticker or the employee ID. E. When conducting penetration testing, the security team will be able to target the desired laptops. Penetration testing is a type of security assessment that simulates a real-world attack on a network or system to identify and exploit vulnerabilities. When conducting penetration testing, the security team will be able to target the desired laptops by using the IP address, hostname, or MAC address of the laptop, not the asset inventory sticker or the employee ID. References = CompTIA Security+ Study Guide (SY0-701), Chapter 1: General Security Concepts, page 17. Professor Messer's CompTIA SY0-701 Security+ Training Course, Section 1.4: Asset Management, video: Asset Inventory (6:12).

NEW QUESTION 38

A company decided to reduce the cost of its annual cyber insurance policy by removing the coverage for ransomware attacks. Which of the following analysis elements did the company most likely use in making this decision?

- A. IMTTR
- B. RTO
- C. ARO
- D. MTBF

Answer: C

Explanation:

ARO (Annualized Rate of Occurrence) is an analysis element that measures the frequency or likelihood of an event happening in a given year. ARO is often used in risk assessment and management, as it helps to estimate the potential loss or impact of an event. A company can use ARO to calculate the annualized loss expectancy (ALE) of an event, which is the product of ARO and the single loss expectancy (SLE). ALE represents the expected cost of an event per year, and can be used to compare with the cost of implementing a security control or purchasing an insurance policy.

The company most likely used ARO in making the decision to remove the coverage for ransomware attacks from its cyber insurance policy. The company may have estimated the ARO of ransomware attacks based on historical data, industry trends, or threat intelligence, and found that the ARO was low or negligible. The company may have also calculated the ALE of ransomware attacks, and found that the ALE was lower than the cost of the insurance policy. Therefore, the company decided to reduce the cost of its annual cyber insurance policy by removing the coverage for ransomware attacks, as it deemed the risk to be acceptable or manageable.

IMTTR (Incident Management Team Training and Readiness), RTO (Recovery Time Objective), and MTBF (Mean Time Between Failures) are not analysis elements that the company most likely used in making the decision to remove the coverage for ransomware attacks from its cyber insurance policy. IMTTR is a process of preparing and training the incident management team to respond effectively to security incidents. IMTTR does not measure the frequency or impact of an event, but rather the capability and readiness of the team. RTO is a metric that defines the maximum acceptable time for restoring a system or service after a disruption. RTO does not measure the frequency or impact of an event, but rather the availability and continuity of the system or service. MTBF is a metric that measures the average time between failures of a system or component. MTBF does not measure the frequency or impact of an event, but rather the reliability and performance of the system or component.

References = CompTIA Security+ SY0-701 Certification Study Guide, page 97-

98; Professor Messer's CompTIA SY0-701 Security+ Training Course, video 5.2 - Risk Management, 0:00 - 3:00.

NEW QUESTION 43

A company's web filter is configured to scan the URL for strings and deny access when matches are found. Which of the following search strings should an analyst employ to prohibit access to non-encrypted websites?

- A. encryption=off\
- B. http://
- C. www*.com
- D. :443

Answer: B

Explanation:

A web filter is a device or software that can monitor, block, or allow web traffic based on predefined rules or policies. One of the common methods of web filtering is to scan the URL for strings and deny access when matches are found. For example, a web filter can block access to websites that contain the words "gambling", "porn", or "malware" in their URLs. A URL is a uniform resource locator that identifies the location and protocol of a web resource. A URL typically consists of the following components: protocol://domain:port/path?query#fragment. The protocol specifies the communication method used to access the web resource, such as HTTP, HTTPS, FTP, or SMTP. The domain is the name of the web server that hosts the web resource, such as www.google.com or www.bing.com. The port is an optional number that identifies the specific service or application running on the web server, such as 80 for HTTP or 443 for HTTPS. The path is the specific folder or file name of the web resource, such as /index.html or /images/logo.png. The query is an optional string that contains additional information or parameters for the web resource, such as ?q=security or ?lang=en. The fragment is an optional string that identifies a specific part or section of the web resource, such as #introduction or #summary.

To prohibit access to non-encrypted websites, an analyst should employ a search string that matches the protocol of non-encrypted web traffic, which is HTTP. HTTP stands for hypertext transfer protocol, and it is a standard protocol for transferring data between web servers and web browsers. However, HTTP does not provide any encryption or security for the data, which means that anyone who intercepts the web traffic can read or modify the data. Therefore, non-encrypted websites are vulnerable to eavesdropping, tampering, or spoofing attacks. To access a non-encrypted website, the URL usually starts with http://, followed by the domain name and optionally the port number. For example, http://www.example.com or http://www.example.com:80. By scanning the URL for the string http://, the web filter can identify and block non-encrypted websites.

The other options are not correct because they do not match the protocol of non-encrypted web traffic. Encryption=off is a possible query string that indicates the encryption status of the web resource, but it is not a standard or mandatory parameter. https:// is the protocol of encrypted web traffic, which uses hypertext transfer protocol secure (HTTPS) to provide encryption and security for the data. www*.com is a possible domain name that matches any website that starts with www and ends with .com, but it does not specify the protocol.

:443 is the port number of HTTPS, which is the protocol of encrypted web traffic. References = CompTIA Security+ Study Guide (SY0-701), Chapter 2: Securing Networks, page 69. Professor Messer's CompTIA SY0-701 Security+ Training Course, Section 2.1: Network Devices and Technologies, video: Web Filter (5:16).

NEW QUESTION 47

After a recent vulnerability scan, a security engineer needs to harden the routers within the corporate network. Which of the following is the most appropriate to disable?

- A. Console access
- B. Routing protocols

- C. VLANs
- D. Web-based administration

Answer: D

Explanation:

Web-based administration is a feature that allows users to configure and manage routers through a web browser interface. While this feature can provide convenience and ease of use, it can also pose a security risk, especially if the web interface is exposed to the internet or uses weak authentication or encryption methods. Web-based administration can be exploited by attackers to gain unauthorized access to the router's settings, firmware, or data, or to launch attacks such as cross-site scripting (XSS) or cross-site request forgery (CSRF). Therefore, disabling web-based administration is a good practice to harden the routers within the corporate network. Console access, routing protocols, and VLANs are other features that can be configured on routers, but they are not the most appropriate to disable for hardening purposes. Console access is a physical connection to the router that requires direct access to the device, which can be secured by locking the router in a cabinet or using a strong password. Routing protocols are essential for routers to exchange routing information and maintain network connectivity, and they can be secured by using authentication or encryption mechanisms. VLANs are logical segments of a network that can enhance network performance and security by isolating traffic and devices, and they can be secured by using VLAN access control lists (VACLs) or private VLANs (PVLANS). References: CCNA SEC: Router Hardening Your Router's Security Stinks: Here's How to Fix It

NEW QUESTION 49

A newly identified network access vulnerability has been found in the OS of legacy IoT devices. Which of the following would best mitigate this vulnerability quickly?

- A. Insurance
- B. Patching
- C. Segmentation
- D. Replacement

Answer: C

Explanation:

Segmentation is a technique that divides a network into smaller subnetworks or segments, each with its own security policies and controls. Segmentation can help mitigate network access vulnerabilities in legacy IoT devices by isolating them from other devices and systems, reducing their attack surface and limiting the potential impact of a breach. Segmentation can also improve network performance and efficiency by reducing congestion and traffic. Patching, insurance, and replacement are other possible strategies to deal with network access vulnerabilities, but they may not be feasible or effective in the short term. Patching may not be available or compatible for legacy IoT devices, insurance may not cover the costs or damages of a cyberattack, and replacement may be expensive and time-consuming. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 142-143

NEW QUESTION 53

A U.S.-based cloud-hosting provider wants to expand its data centers to new international locations. Which of the following should the hosting provider consider first?

- A. Local data protection regulations
- B. Risks from hackers residing in other countries
- C. Impacts to existing contractual obligations
- D. Time zone differences in log correlation

Answer: A

Explanation:

Local data protection regulations are the first thing that a cloud-hosting provider should consider before expanding its data centers to new international locations. Data protection regulations are laws or standards that govern how personal or sensitive data is collected, stored, processed, and transferred across borders. Different countries or regions may have different data protection regulations, such as the General Data Protection Regulation (GDPR) in the European Union, the Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada, or the California Consumer Privacy Act (CCPA) in the United States. A cloud-hosting provider must comply with the local data protection regulations of the countries or regions where it operates or serves customers, or else it may face legal penalties, fines, or reputational damage. Therefore, a cloud-hosting provider should research and understand the local data protection regulations of the new international locations before expanding its data centers there. References = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 7, page 269. CompTIA Security+ SY0-701 Exam Objectives, Domain 5.1, page 14.

NEW QUESTION 58

A company needs to provide administrative access to internal resources while minimizing the traffic allowed through the security boundary. Which of the following methods is most secure?

- A. Implementing a bastion host
- B. Deploying a perimeter network
- C. Installing a WAF
- D. Utilizing single sign-on

Answer: A

Explanation:

A bastion host is a special-purpose server that is designed to withstand attacks and provide secure access to internal resources. A bastion host is usually placed on the edge of a network, acting as a gateway or proxy to the internal network. A bastion host can be configured to allow only certain types of traffic, such as SSH or HTTP, and block all other traffic. A bastion host can also run security software such as firewalls, intrusion detection systems, and antivirus programs to monitor and filter incoming and outgoing traffic. A bastion host can provide administrative access to internal resources by requiring strong authentication and encryption, and by logging all activities for auditing purposes¹².

A bastion host is the most secure method among the given options because it minimizes the traffic allowed through the security boundary and provides a single point of control and defense. A bastion host can also isolate the internal network from direct exposure to the internet or other untrusted networks, reducing the attack surface and the risk of compromise³.

Deploying a perimeter network is not the correct answer, because a perimeter network is a network segment that separates the internal network from the external network. A perimeter network usually hosts public-facing services such as web servers, email servers, or DNS servers that need to be accessible from the internet. A perimeter network does not provide administrative access to internal resources, but rather protects them from unauthorized access. A perimeter network can

also increase the complexity and cost of network management and security⁴.

Installing a WAF is not the correct answer, because a WAF is a security tool that protects web applications from common web-based attacks by monitoring, filtering, and blocking HTTP traffic. A WAF can prevent attacks such as cross-site scripting, SQL injection, or file inclusion, among others. A WAF does not provide administrative access to internal resources, but rather protects them from web application vulnerabilities. A WAF is also not a comprehensive solution for network security, as it only operates at the application layer and does not protect against other types of attacks or threats⁵.

Utilizing single sign-on is not the correct answer, because single sign-on is a method of authentication that allows users to access multiple sites, services, or applications with one username and password. Single sign-on can simplify the sign-in process for users and reduce the number of passwords they have to remember and manage. Single sign-on does not provide administrative access to internal resources, but rather enables access to various resources that the user is authorized to use. Single sign-on can also introduce security risks if the user's credentials are compromised or if the single sign-on provider is breached⁶. References = 1: Bastion host - Wikipedia, 2: 14 Best Practices to Secure SSH Bastion Host - goteleport.com, 3: The Importance Of Bastion Hosts In Network

Security, 4: What is the network perimeter? | Cloudflare, 5: What is a WAF? | Web Application Firewall explained, 6: [What is single sign-on (SSO)? - Definition from WhatIs.com]

NEW QUESTION 60

An employee receives a text message that appears to have been sent by the payroll department and is asking for credential verification. Which of the following social engineering techniques are being attempted? (Choose two.)

- A. Typosquatting
- B. Phishing
- C. Impersonation
- D. Vishing
- E. Smishing
- F. Misinformation

Answer: BE

Explanation:

Smishing is a type of social engineering technique that uses text messages (SMS) to trick victims into revealing sensitive information, clicking malicious links, or downloading malware. Smishing messages often appear to come from legitimate sources, such as banks, government agencies, or service providers, and use urgent or threatening language to persuade the recipients to take action¹². In this scenario, the text message that claims to be from the payroll department is an example of smishing.

Impersonation is a type of social engineering technique that involves pretending to be someone else, such as an authority figure, a trusted person, or a colleague, to gain the trust or cooperation of the target. Impersonation can be done through various channels, such as phone calls, emails, text messages, or in-person visits, and can be used to obtain information, access, or money from the victim³⁴. In this scenario, the text message that pretends to be from the payroll department is an example of impersonation.

* A. Typosquatting is a type of cyberattack that involves registering domain names that are similar to popular or well-known websites, but with intentional spelling errors or different extensions. Typosquatting aims to exploit the common mistakes that users make when typing web addresses, and redirect them to malicious or fraudulent sites that may steal their information, install malware, or display ads⁵⁶. Typosquatting is not related to text messages or credential verification.

* B. Phishing is a type of social engineering technique that uses fraudulent emails to trick recipients into revealing sensitive information, clicking malicious links, or downloading malware. Phishing emails often mimic the appearance and tone of legitimate organizations, such as banks, retailers, or service providers, and use deceptive or urgent language to persuade the recipients to take action⁷⁸. Phishing is not related to text messages or credential verification.

* D. Vishing is a type of social engineering technique that uses voice calls to trick victims into revealing sensitive information, such as passwords, credit card numbers, or bank account details. Vishing calls often appear to come from legitimate sources, such as law enforcement, government agencies, or technical support, and use scare tactics or false promises to persuade the recipients to comply⁹. Vishing is not related to text messages or credential verification.

* F. Misinformation is a type of social engineering technique that involves spreading false or misleading information to influence the beliefs, opinions, or actions of the target. Misinformation can be used to manipulate public perception, create confusion, damage reputation, or promote an agenda. Misinformation is not related to text messages or credential verification.

References = 1: What is Smishing? | Definition and Examples | Kaspersky 2: Smishing - Wikipedia 3: Impersonation Attacks: What Are They and How Do You Protect Against

Them? 4: Impersonation - Wikipedia 5: What is Typosquatting? | Definition and Examples | Kaspersky 6: Typosquatting - Wikipedia 7: What is Phishing? | Definition and Examples | Kaspersky 8: Phishing - Wikipedia 9: What is Vishing? | Definition and Examples | Kaspersky : Vishing - Wikipedia : What is Misinformation? | Definition and Examples | Britannica : Misinformation - Wikipedia

NEW QUESTION 62

A company is developing a business continuity strategy and needs to determine how many staff members would be required to sustain the business in the case of a disruption. Which of the following best describes this step?

- A. Capacity planning
- B. Redundancy
- C. Geographic dispersion
- D. Tablet exercise

Answer: A

Explanation:

Capacity planning is the process of determining the resources needed to meet the current and future demands of an organization. Capacity planning can help a company develop a business continuity strategy by estimating how many staff members would be required to sustain the business in the case of a disruption, such as a natural disaster, a cyberattack, or a pandemic. Capacity planning can also help a company optimize the use of its resources, reduce costs, and improve performance. References = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 4, page 184. CompTIA Security+ (SY0-701) Certification Exam Objectives, Domain 4.1, page 14. Business Continuity – SY0-601 CompTIA Security+ : 4.1

NEW QUESTION 67

Which of the following has been implemented when a host-based firewall on a legacy Linux system allows connections from only specific internal IP addresses?

- A. Compensating control
- B. Network segmentation
- C. Transfer of risk
- D. SNMP traps

Answer: A

Explanation:

A compensating control is a security measure that is implemented to mitigate the risk of a vulnerability or a weakness that cannot be resolved by the primary control. A compensating control does not prevent or eliminate the vulnerability or weakness, but it can reduce the likelihood or impact of an attack. A host-based firewall on a legacy Linux system that allows connections from only specific internal IP addresses is an example of a compensating control, as it can limit the exposure of the system to potential threats from external or unauthorized sources. A host-based firewall is a software application that monitors and filters the incoming and outgoing network traffic on a single host, based on a set of rules or policies. A legacy Linux system is an older version of the Linux operating system that may not be compatible with the latest security updates or patches, and may have known vulnerabilities or weaknesses that could be exploited by attackers. References = Security Controls – SY0-601 CompTIA Security+ : 5.1, Security Controls – CompTIA Security+ SY0-501 – 5.7, CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 5, page 240. CompTIA Security+ (SY0-701) Certification Exam Objectives, Domain 5.1, page 18.

NEW QUESTION 69

A technician wants to improve the situational and environmental awareness of existing users as they transition from remote to in-office work. Which of the following is the best option?

- A. Send out periodic security reminders.
- B. Update the content of new hire documentation.
- C. Modify the content of recurring training.
- D. Implement a phishing campaign.

Answer: C

Explanation:

Recurring training is a type of security awareness training that is conducted periodically to refresh and update the knowledge and skills of the users. Recurring training can help improve the situational and environmental awareness of existing users as they transition from remote to in-office work, as it can cover the latest threats, best practices, and policies that are relevant to their work environment. Modifying the content of recurring training can ensure that the users are aware of the current security landscape and the expectations of their roles. References = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 5, page 232. CompTIA Security+ (SY0-701) Certification Exam Objectives, Domain 5.1, page 18.

NEW QUESTION 70

After a security incident, a systems administrator asks the company to buy a NAC platform. Which of the following attack surfaces is the systems administrator trying to protect?

- A. Bluetooth
- B. Wired
- C. NFC
- D. SCADA

Answer: B

Explanation:

A NAC (network access control) platform is a technology that enforces security policies on devices that attempt to access a network. A NAC platform can verify the identity, role, and compliance of the devices, and grant or deny access based on predefined rules. A NAC platform can protect both wired and wireless networks, but in this scenario, the systems administrator is trying to protect the wired attack surface, which is the set of vulnerabilities that can be exploited through a physical connection to the network.

References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 5, page 189; CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 5, page 237.

NEW QUESTION 73

A security analyst scans a company's public network and discovers a host is running a remote desktop that can be used to access the production network. Which of the following changes should the security analyst recommend?

- A. Changing the remote desktop port to a non-standard number
- B. Setting up a VPN and placing the jump server inside the firewall
- C. Using a proxy for web connections from the remote desktop server
- D. Connecting the remote server to the domain and increasing the password length

Answer: B

Explanation:

A VPN is a virtual private network that creates a secure tunnel between two or more devices over a public network. A VPN can encrypt and authenticate the data, as well as hide the IP addresses and locations of the devices. A jump server is a server that acts as an intermediary between a user and a target server, such as a production server. A jump server can provide an additional layer of security and access control, as well as logging and auditing capabilities. A firewall is a device or software that filters and blocks unwanted network traffic based on predefined rules. A firewall can protect the internal network from external threats and limit the exposure of sensitive services and ports. A security analyst should recommend setting up a VPN and placing the jump server inside the firewall to improve the security of the remote desktop access to the production network. This way, the remote desktop service will not be exposed to the public network, and only authorized users with VPN credentials can access the jump server and then the production

server. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 8: Secure Protocols and Services, page 382-383 1; Chapter 9: Network Security, page 441-442 1

NEW QUESTION 74

Which of the following best practices gives administrators a set period to perform changes to an operational system to ensure availability and minimize business impacts?

- A. Impact analysis
- B. Scheduled downtime

- C. Backout plan
- D. Change management boards

Answer: B

Explanation:

Scheduled downtime is a planned period of time when a system or service is unavailable for maintenance, updates, upgrades, or other changes. Scheduled downtime gives administrators a set period to perform changes to an operational system without disrupting the normal business operations or affecting the availability of the system or service. Scheduled downtime also allows administrators to inform the users and stakeholders about the expected duration and impact of the changes. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 12: Security Operations and Administration, page 579 1

NEW QUESTION 75

Which of the following is used to quantitatively measure the criticality of a vulnerability?

- A. CVE
- B. CVSS
- C. CIA
- D. CERT

Answer: B

Explanation:

CVSS stands for Common Vulnerability Scoring System, which is a framework that provides a standardized way to assess and communicate the severity and risk of vulnerabilities. CVSS uses a set of metrics and formulas to calculate a numerical score ranging from 0 to 10, where higher scores indicate higher criticality. CVSS can help organizations prioritize remediation efforts and compare vulnerabilities across different systems and vendors. The other options are not used to measure the criticality of a vulnerability, but rather to identify, classify, or report them. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 39

NEW QUESTION 79

During a security incident, the security operations team identified sustained network traffic from a malicious IP address: 10.1.4.9. A security analyst is creating an inbound firewall rule to block the IP address from accessing the organization's network. Which of the following fulfills this request?

- A. access-list inbound deny ig source 0.0.0.0/0 destination 10.1.4.9/32
- B. access-list inbound deny ig source 10.1.4.9/32 destination 0.0.0.0/0
- C. access-list inbound permit ig source 10.1.4.9/32 destination 0.0.0.0/0
- D. access-list inbound permit ig source 0.0.0.0/0 destination 10.1.4.9/32

Answer: B

Explanation:

A firewall rule is a set of criteria that determines whether to allow or deny a packet to pass through the firewall. A firewall rule consists of several elements, such as the action, the protocol, the source address, the destination address, and the port number. The syntax of a firewall rule may vary depending on the type and vendor of the firewall, but the basic logic is the same. In this question, the security analyst is creating an inbound firewall rule to block the IP address 10.1.4.9 from accessing the organization's network. This means that the action should be deny, the protocol should be any (or ig for IP), the source address should be 10.1.4.9/32 (which means a single IP address), the destination address should be 0.0.0.0/0 (which means any IP address), and the port number should be any. Therefore, the correct firewall rule is:

```
access-list inbound deny ig source 10.1.4.9/32 destination 0.0.0.0/0
```

This rule will match any packet that has the source IP address of 10.1.4.9 and drop it. The other options are incorrect because they either have the wrong action, the wrong source address, or the wrong destination address. For example, option A has the source and destination addresses reversed, which means that it will block any packet that has the destination IP address of 10.1.4.9, which is not the intended goal. Option C has the wrong action, which is permit, which means that it will allow the packet to pass through the firewall, which is also not the intended goal. Option D has the same problem as option A, with the source and destination addresses reversed.

References = Firewall Rules – CompTIA Security+ SY0-401: 1.2, Firewalls – SY0-601 CompTIA Security+ : 3.3, Firewalls – CompTIA Security+ SY0-501, Understanding Firewall Rules – CompTIA Network+ N10-005: 5.5, Configuring Windows Firewall – CompTIA A+ 220-1102 – 1.6.

NEW QUESTION 83

An enterprise has been experiencing attacks focused on exploiting vulnerabilities in older browser versions with well-known exploits. Which of the following security solutions should be configured to best provide the ability to monitor and block these known signature-based attacks?

- A. ACL
- B. DLP
- C. IDS
- D. IPS

Answer: D

Explanation:

An intrusion prevention system (IPS) is a security device that monitors network traffic and blocks or modifies malicious packets based on predefined rules or signatures. An IPS can prevent attacks that exploit known vulnerabilities in older browser versions by detecting and dropping the malicious packets before they reach the target system. An IPS can also perform other functions, such as rate limiting, encryption, or redirection. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 3: Securing Networks, page 132.

NEW QUESTION 85

An attacker posing as the Chief Executive Officer calls an employee and instructs the employee to buy gift cards. Which of the following techniques is the attacker using?

- A. Smishing
- B. Disinformation
- C. Impersonating

D. Whaling

Answer: D

Explanation:

Whaling is a type of phishing attack that targets high-profile individuals, such as executives, celebrities, or politicians. The attacker impersonates someone with authority or influence and tries to trick the victim into performing an action, such as transferring money, revealing sensitive information, or clicking on a malicious link. Whaling is also called CEO fraud or business email compromise2.

References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 3, page 97.

NEW QUESTION 87

Which of the following is a hardware-specific vulnerability?

- A. Firmware version
- B. Buffer overflow
- C. SQL injection
- D. Cross-site scripting

Answer: A

Explanation:

Firmware is a type of software that is embedded in a hardware device, such as a router, a printer, or a BIOS chip. Firmware controls the basic functions and operations of the device, and it can be updated or modified by the manufacturer or the user. Firmware version is a hardware-specific vulnerability, as it can expose the device to security risks if it is outdated, corrupted, or tampered with. An attacker can exploit firmware vulnerabilities to gain unauthorized access, modify device settings, install malware, or cause damage to the device or the network. Therefore, it is important to keep firmware updated and verify its integrity and authenticity.

References = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 2, page 67. CompTIA Security+ SY0-701 Exam Objectives, Domain 2.1, page 10.

NEW QUESTION 90

The marketing department set up its own project management software without telling the appropriate departments. Which of the following describes this scenario?

- A. Shadow IT
- B. Insider threat
- C. Data exfiltration
- D. Service disruption

Answer: A

Explanation:

Shadow IT is the term used to describe the use of unauthorized or unapproved IT resources within an organization. The marketing department set up its own project management software without telling the appropriate departments, such as IT, security, or compliance. This could pose a risk to the organization's security posture, data integrity, and regulatory compliance1.

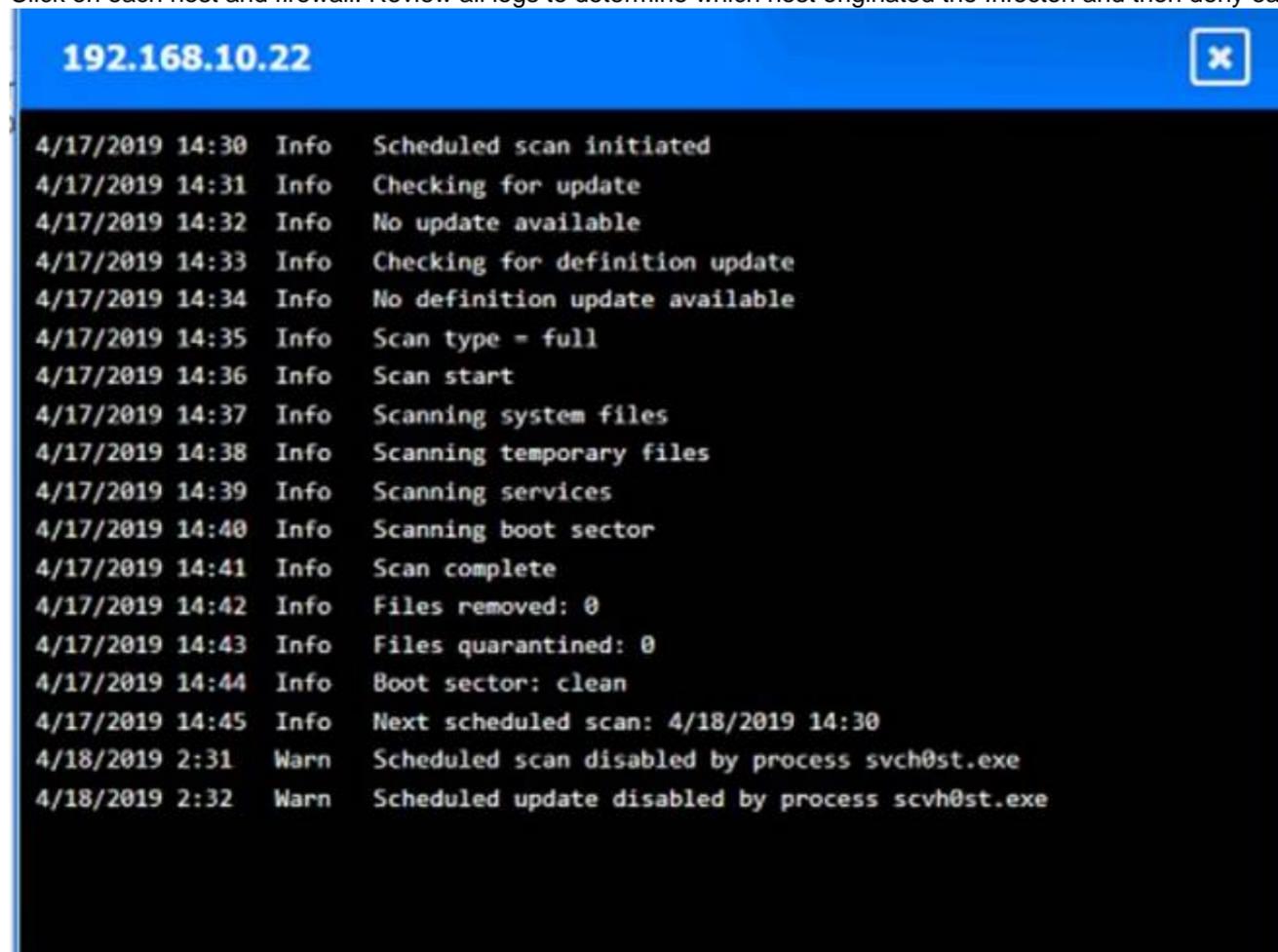
References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 2, page 35.

NEW QUESTION 91

HOTSPOT

You are security administrator investigating a potential infection on a network.

Click on each host and firewall. Review all logs to determine which host originated the Infection and then deny each remaining hosts clean or infected.



```

192.168.10.37
4/17/2019 14:30 Info Scheduled scan initiated
4/17/2019 14:31 Info Checking for update
4/17/2019 14:32 Info No update available
4/17/2019 14:33 Info Checking for definition update
4/17/2019 14:34 Info No definition update available
4/17/2019 14:35 Info Scan type = full
4/17/2019 14:36 Info Scan start
4/17/2019 14:37 Info Scanning system files
4/17/2019 14:38 Info Scanning temporary files
4/17/2019 14:39 Info Scanning services
4/17/2019 14:40 Info Scanning boot sector
4/17/2019 14:41 Info Scan complete
4/17/2019 14:42 Info Files removed: 0
4/17/2019 14:43 Info Files quarantined: 0
4/17/2019 14:44 Info Boot sector: clean
4/17/2019 14:45 Info Next scheduled scan: 4/18/2019 14:30
4/18/2019 14:30 Info Scheduled scan initiated
4/18/2019 14:31 Info Checking for update
4/18/2019 14:32 Info No update available
4/18/2019 14:33 Info Checking for definition update
4/18/2019 14:34 Info Update available v10.2.3.4440
4/18/2019 14:33 Info Downloading update
4/18/2019 14:35 Info Definition update complete
4/18/2019 14:35 Info Scan type = full
4/18/2019 14:36 Info Scan start
4/18/2019 14:37 Info Scanning system files
4/18/2019 14:37 Warn File found svch0st.exe match definition v10.2.3.4440
4/18/2019 14:37 Warn File quarantined svch0st.exe
4/18/2019 14:38 Info Scanning temporary files
4/18/2019 14:39 Info Scanning services
4/18/2019 14:40 Info Scanning boot sector
4/18/2019 14:41 Info Scan complete
4/18/2019 14:42 Info Files removed: 0
4/18/2019 14:43 Info Files quarantined: 0
4/18/2019 14:44 Info Boot sector: clean
4/18/2019 14:45 Info Next scheduled scan: 4/19/2019 14:30

```

```

192.168.10.41
4/17/2019 14:30 Info Scan start
4/17/2019 14:37 Info Scanning system files
4/17/2019 14:38 Info Scanning temporary files
4/17/2019 14:39 Info Scanning services
4/17/2019 14:40 Info Scanning boot sector
4/17/2019 14:41 Info Scan complete
4/17/2019 14:42 Info Files removed: 0
4/17/2019 14:43 Info Files quarantined: 0
4/17/2019 14:44 Info Boot sector: clean
4/17/2019 14:45 Info Next scheduled scan: 4/18/2019 14:30
4/18/2019 14:30 Info Scheduled scan initiated
4/18/2019 14:31 Info Checking for update
4/18/2019 14:32 Info No update available
4/18/2019 14:33 Info Checking for definition update
4/18/2019 14:34 Error Unable to reach update server
4/18/2019 14:35 Info Scan type = full
4/18/2019 14:36 Info Scan start
4/18/2019 14:37 Info Scanning system files
4/18/2019 14:37 Warn File svch0st.exe match heuristic pattern 0c09488c08d0f3k
4/18/2019 14:37 Error Unable to quarantine file svch0st.exe
4/18/2019 14:38 Info Scanning temporary files
4/18/2019 14:39 Info Scanning services
4/18/2019 14:40 Info Scanning boot sector
4/18/2019 14:41 Info Scan complete
4/18/2019 14:42 Info Files removed: 0
4/18/2019 14:43 Info Files quarantined: 0
4/18/2019 14:43 Warn File quarantine file
4/18/2019 14:44 Info Boot sector: clean
4/18/2019 14:45 Info Next scheduled scan: 4/19/2019 14:30

```

Firewall							
Timestamp	Source	Destination	Destination Port	Application	Action	Client Bytes	Server Bytes
4/17/2019 16:01:44	10.10.9.18	57.203.54.183	443	ssl	Permit	6953	99427
4/17/2019 16:01:58	192.168.10.37	57.203.54.221	443	ssl	Permit	9301	199386
4/17/2019 16:17:06	192.168.10.22	10.10.9.12	135	rpc	Permit	175	1504
4/17/2019 16:27:36	192.168.10.41	10.10.9.12	445	smbv1	Permit	345	34757
4/17/2019 16:28:06	10.10.9.12	192.168.10.41	135	rpc	Permit	754	4771
4/17/2019 16:33:31	10.10.9.18	192.168.10.22	135	rpc	Permit	643	2355
4/17/2019 16:35:36	192.168.10.37	10.10.9.12	135	smbv2	Permit	649	5644
4/17/2019 23:58:36	10.10.9.12	192.168.10.41		icmp	Permit	128	128
4/17/2019 23:58:43	10.10.9.12	192.168.10.22		icmp	Permit	128	128
4/17/2019 23:58:45	10.10.9.12	192.168.10.37		icmp	Permit	128	128
4/18/2019 2:31:36	10.10.9.18	192.168.10.41	445	smbv2	Permit	1874	23874
4/18/2019 2:31:45	192.168.10.22	57.203.55.29	8080	http	Permit	7203	75997
4/18/2019 2:31:51	10.10.9.18	57.203.56.201	443	ssl	Permit	9953	199730
4/18/2019 2:31:02	192.168.10.22	57.203.55.234	443	http	Permit	4937	84937
4/18/2019 2:39:11	192.168.10.41	57.203.53.89	8080	http	Permit	8201	133183
4/18/2019 2:39:12	10.10.9.18	57.203.55.19	8080	ssl	Permit	1284	9102854
4/18/2019 2:39:32	192.168.10.37	57.203.56.113	443	ssl	Permit	9341	9938
4/18/2019 13:37:36	192.168.10.22	10.10.9.18	445	smbv3	Permit	1874	23874
4/18/2019 13:39:43	192.168.10.22	10.10.9.18	135	rpc	Permit	673	41358
4/18/2019 13:45:04	10.10.9.18	192.168.10.37	135	rpc	Permit	693	1952
4/18/2019 13:47:44	10.10.9.12	192.168.10.41	445	smbv3	Permit	482	3505
4/18/2019 13:52:57	10.10.9.18	192.168.10.22	135	rpc	Permit	545	9063
4/18/2019 13:53:01	192.168.10.37	10.10.9.12	335	smbv3	Permit	876	8068
4/18/2019 14:30:04	10.10.9.12	57.203.56.231	443	ssl	Permit	9901	199730
4/18/2019 14:30:04	192.168.10.37	57.203.56.143	443	ssl	Permit	10092	209938

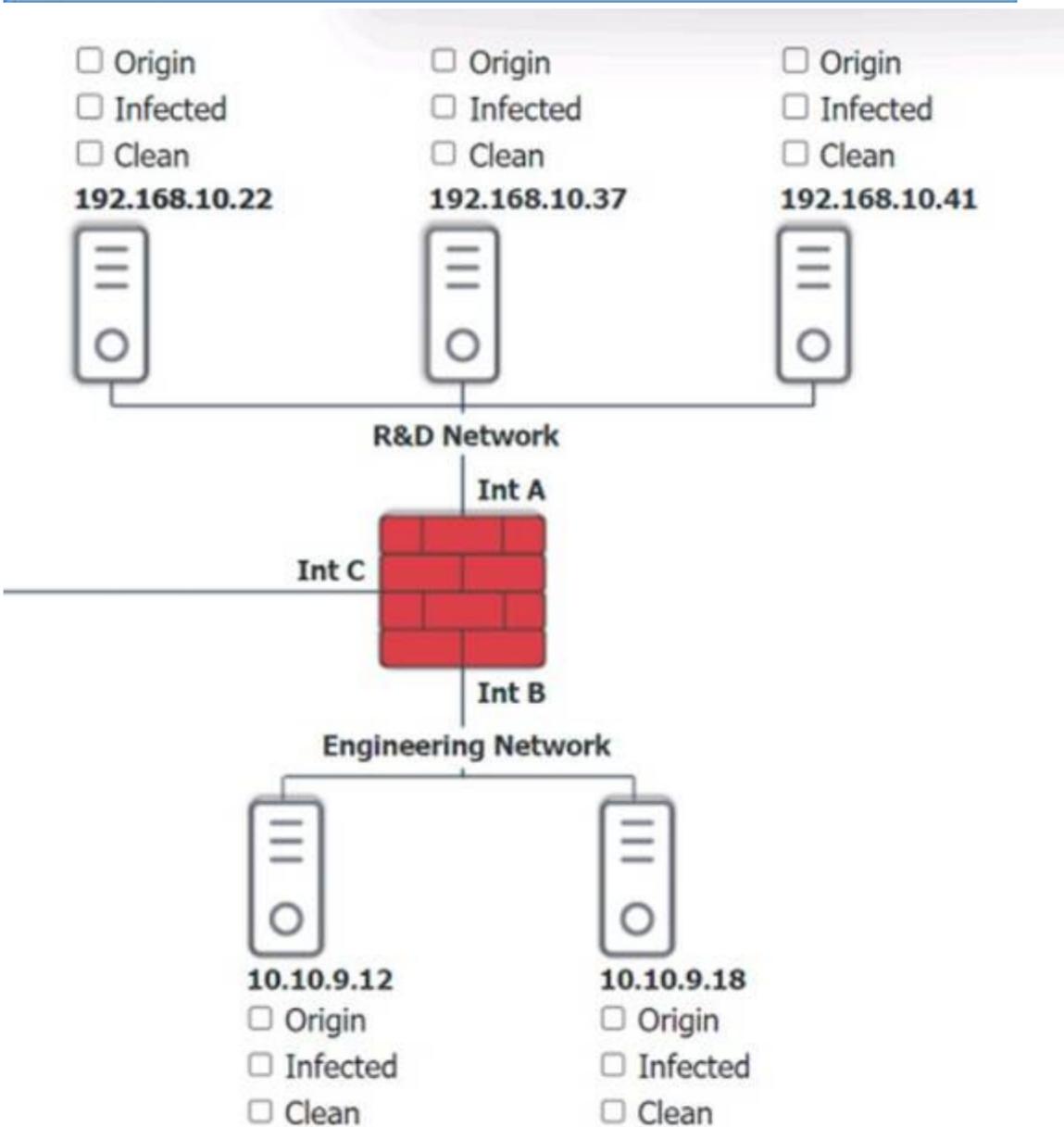
```

10.10.9.12
4/17/2019 14:30 Info Scheduled scan initiated
4/17/2019 14:31 Info Checking for update
4/17/2019 14:32 Info No update available
4/17/2019 14:33 Info Checking for definition update
4/17/2019 14:34 Info No definition update available
4/17/2019 14:35 Info Scan type = full
4/17/2019 14:36 Info Scan start
4/17/2019 14:37 Info Scanning system files
4/17/2019 14:38 Info Scanning temporary files
4/17/2019 14:39 Info Scanning services
4/17/2019 14:40 Info Scanning boot sector
4/17/2019 14:41 Info Scan complete
4/17/2019 14:42 Info Files removed: 0
4/17/2019 14:43 Info Files quarantined: 0
4/17/2019 14:44 Info Boot sector: clean
4/17/2019 14:45 Info Next scheduled scan: 4/18/2019 14:30
4/18/2019 14:30 Info Scheduled scan initiated
4/18/2019 14:31 Info Checking for update
4/18/2019 14:32 Info No update available
4/18/2019 14:33 Info Checking for definition update
4/18/2019 14:34 Info Update available v10.2.3.4440
4/18/2019 14:33 Info Downloading update
4/18/2019 14:35 Info Definition update complete
4/18/2019 14:35 Info Scan type = full
4/18/2019 14:36 Info Scan start
4/18/2019 14:37 Info Scanning system files
4/18/2019 14:37 Warn File found svchost.exe match definition v10.2.3.4440
4/18/2019 14:37 Warn File quarantined svchost.exe
4/18/2019 14:38 Info Scanning temporary files
4/18/2019 14:39 Info Scanning services

```

```

10.10.9.18
4/17/2019 14:30 Info Scheduled scan initiated
4/17/2019 14:31 Info Checking for update
4/17/2019 14:32 Info No update available
4/17/2019 14:33 Info Checking for definition update
4/17/2019 14:34 Info No definition update available
4/17/2019 14:35 Info Scan type = full
4/17/2019 14:36 Info Scan start
4/17/2019 14:37 Info Scanning system files
4/17/2019 14:38 Info Scanning temporary files
4/17/2019 14:39 Info Scanning services
4/17/2019 14:40 Info Scanning boot sector
4/17/2019 14:41 Info Scan complete
4/17/2019 14:42 Info Files removed: 0
4/17/2019 14:43 Info Files quarantined: 0
4/17/2019 14:44 Info Boot sector: clean
4/17/2019 14:45 Info Next scheduled scan: 4/18/2019 14:30
4/18/2019 14:30 Info Scheduled scan initiated
4/18/2019 14:31 Info Checking for update
4/18/2019 14:32 Info No update available
4/18/2019 14:33 Info Checking for definition update
4/18/2019 14:34 Error Unable to reach update server
4/18/2019 14:35 Info Scan type = full
4/18/2019 14:36 Info Scan start
4/18/2019 14:37 Info Scanning system files
4/18/2019 14:37 Warn File svchost.exe match heuristic pattern 0c09488c08d0f3k
4/18/2019 14:37 Error Unable to quarantine file svchost.exe
4/18/2019 14:38 Info Scanning temporary files
4/18/2019 14:39 Info Scanning services
4/18/2019 14:40 Info Scanning boot sector
4/18/2019 14:41 Info Scan complete
  
```



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Based on the logs, it seems that the host that originated the infection is 192.168.10.22. This host has a suspicious process named svchost.exe running on port 443, which is unusual for a Windows service. It also has a large number of outbound connections to different IP addresses on port 443, indicating that it is part of a

botnet.

The firewall log shows that this host has been communicating with 10.10.9.18, which is another infected host on the engineering network. This host also has a suspicious process named svchost.exe running on port 443, and a large number of outbound connections to different IP addresses on port 443. The other hosts on the R&D network (192.168.10.37 and 192.168.10.41) are clean, as they do not have any suspicious processes or connections.

NEW QUESTION 94

A company's marketing department collects, modifies, and stores sensitive customer data. The infrastructure team is responsible for securing the data while in transit and at rest. Which of the following data roles describes the customer?

- A. Processor
- B. Custodian
- C. Subject
- D. Owner

Answer: C

Explanation:

According to the CompTIA Security+ SY0-701 Certification Study Guide, data subjects are the individuals whose personal data is collected, processed, or stored by an organization. Data subjects have certain rights and expectations regarding how their data is handled, such as the right to access, correct, delete, or restrict their data. Data subjects are different from data owners, who are the individuals or entities that have the authority and responsibility to determine how data is classified, protected, and used. Data subjects are also different from data processors, who are the individuals or entities that perform operations on data on behalf of the data owner, such as collecting, modifying, storing, or transmitting data. Data subjects are also different from data custodians, who are the individuals or entities that implement the security controls and procedures specified by the data owner to protect data while in transit and at rest.

References: CompTIA Security+ SY0-701 Certification Study Guide, Chapter 2: Data Security, page 511

NEW QUESTION 96

A security manager created new documentation to use in response to various types of security incidents. Which of the following is the next step the manager should take?

- A. Set the maximum data retention policy.
- B. Securely store the documents on an air-gapped network.
- C. Review the documents' data classification policy.
- D. Conduct a tabletop exercise with the team.

Answer: D

Explanation:

A tabletop exercise is a simulated scenario that tests the effectiveness of a security incident response plan. It involves gathering the relevant stakeholders and walking through the steps of the plan, identifying any gaps or issues that need to be addressed. A tabletop exercise is a good way to validate the documentation created by the security manager and ensure that the team is prepared for various types of security incidents. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 6: Risk Management, page 2841. CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 6: Risk Management, page 2842.

NEW QUESTION 98

An organization recently updated its security policy to include the following statement:

Regular expressions are included in source code to remove special characters such as \$, |, ;, &, ` , and ? from variables set by forms in a web application.

Which of the following best explains the security technique the organization adopted by making this addition to the policy?

- A. Identify embedded keys
- B. Code debugging
- C. Input validation
- D. Static code analysis

Answer: C

Explanation:

Input validation is a security technique that checks the user input for any malicious or unexpected data before processing it by the application. Input validation can prevent various types of attacks, such as injection, cross-site scripting, buffer overflow, and command execution, that exploit the vulnerabilities in the application code. Input validation can be performed on both the client-side and the server-side, using methods such as whitelisting, blacklisting, filtering, sanitizing, escaping, and encoding. By including regular expressions in the source code to remove special characters from the variables set by the forms in the web application, the organization adopted input validation as a security technique. Regular expressions are patterns that match a specific set of characters or strings, and can be used to filter out any unwanted or harmful input. Special characters, such as \$, |, ;, &, ` , and ? , can be used by attackers to inject commands or scripts into the application, and cause damage or data theft. By removing these characters from the input, the organization can reduce the risk of such attacks.

Identify embedded keys, code debugging, and static code analysis are not the security techniques that the organization adopted by making this addition to the policy. Identify embedded keys is a process of finding and removing any hard-coded keys or credentials from the source code, as these can pose a security risk if exposed or compromised. Code debugging is a process of finding and fixing any errors or bugs in the source code, which can affect the functionality or performance of the application. Static code analysis is a process of analyzing the source code without executing it, to identify any vulnerabilities, flaws, or coding standards violations. These techniques are not related to the use of regular expressions to remove special characters from the input.

References = CompTIA Security+ SY0-701 Certification Study Guide, page 375-376; Professor Messer's CompTIA SY0-701 Security+ Training Course, video 4.1 - Vulnerability Scanning, 8:00 - 9:08; Application Security – SY0-601 CompTIA Security+ : 3.2, 0:00 - 2:00.

NEW QUESTION 99

A security administrator is deploying a DLP solution to prevent the exfiltration of sensitive customer data. Which of the following should the administrator do first?

- A. Block access to cloud storage websites.
- B. Create a rule to block outgoing email attachments.
- C. Apply classifications to the data.
- D. Remove all user permissions from shares on the file server.

Answer: C

Explanation:

Data classification is the process of assigning labels or tags to data based on its sensitivity, value, and risk. Data classification is the first step in a data loss prevention (DLP) solution, as it helps to identify what data needs to be protected and how. By applying classifications to the data, the security administrator can define appropriate policies and rules for the DLP solution to prevent the exfiltration of sensitive customer data. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 8: Data Protection, page 323. CompTIA Security+ Practice Tests: Exam SY0-701, 3rd Edition, Chapter 8: Data Protection, page 327.

NEW QUESTION 102

Which of the following would be the best way to handle a critical business application that is running on a legacy server?

- A. Segmentation
- B. Isolation
- C. Hardening
- D. Decommissioning

Answer: C

Explanation:

A legacy server is a server that is running outdated or unsupported software or hardware, which may pose security risks and compatibility issues. A critical business application is an application that is essential for the operation and continuity of the business, such as accounting, payroll, or inventory management. A legacy server running a critical business application may be difficult to replace or upgrade, but it should not be left unsecured or exposed to potential threats. One of the best ways to handle a legacy server running a critical business application is to harden it. Hardening is the process of applying security measures and configurations to a system to reduce its attack surface and vulnerability. Hardening a legacy server may involve steps such as:

- ? Applying patches and updates to the operating system and the application, if available
 - ? Removing or disabling unnecessary services, features, or accounts
 - ? Configuring firewall rules and network access control lists to restrict inbound and outbound traffic
 - ? Enabling encryption and authentication for data transmission and storage
 - ? Implementing logging and monitoring tools to detect and respond to anomalous or malicious activity
 - ? Performing regular backups and testing of the system and the application
- Hardening a legacy server can help protect the critical business application from unauthorized access, modification, or disruption, while maintaining its functionality and availability. However, hardening a legacy server is not a permanent solution, and it may not be sufficient to address all the security issues and challenges posed by the outdated or unsupported system. Therefore, it is advisable to plan for the eventual decommissioning or migration of the legacy server to a more secure and modern platform, as soon as possible. References: CompTIA Security+ SY0-701 Certification Study Guide, Chapter 3: Architecture and Design, Section 3.2: Secure System Design, Page 133 1; CompTIA Security+ Certification Exam Objectives, Domain 3: Architecture and Design, Objective 3.2: Explain the importance of secure system design, Subobjective: Legacy systems 2

NEW QUESTION 107

A company is discarding a classified storage array and hires an outside vendor to complete the disposal. Which of the following should the company request from the vendor?

- A. Certification
- B. Inventory list
- C. Classification
- D. Proof of ownership

Answer: A

Explanation:

The company should request a certification from the vendor that confirms the storage array has been disposed of securely and in compliance with the company's policies and standards. A certification provides evidence that the vendor has followed the proper procedures and methods to destroy the classified data and prevent unauthorized access or recovery. A certification may also include details such as the date, time, location, and method of disposal, as well as the names and signatures of the personnel involved. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 3, page 1441

NEW QUESTION 111

During the onboarding process, an employee needs to create a password for an intranet account. The password must include ten characters, numbers, and letters, and two special characters. Once the password is created, the company will grant the employee access to other company-owned websites based on the intranet profile. Which of the following access management concepts is the company most likely using to safeguard intranet accounts and grant access to multiple sites based on a user's intranet account? (Select two).

- A. Federation
- B. Identity proofing
- C. Password complexity
- D. Default password changes
- E. Password manager
- F. Open authentication

Answer: AC

Explanation:

Federation is an access management concept that allows users to authenticate once and access multiple resources or services across different domains or organizations. Federation relies on a trusted third party that stores the user's credentials and provides them to the requested resources or services without exposing them. Password complexity is a security measure that requires users to create passwords that meet certain criteria, such as length, character types, and uniqueness. Password complexity can help prevent brute-force attacks, password guessing, and credential stuffing by making passwords harder to crack or guess. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 308-309 and 312-313 1

NEW QUESTION 113

An organization is leveraging a VPN between its headquarters and a branch location. Which of the following is the VPN protecting?

- A. Data in use
- B. Data in transit
- C. Geographic restrictions
- D. Data sovereignty

Answer: B

Explanation:

Data in transit is data that is moving from one location to another, such as over a network or through the air. Data in transit is vulnerable to interception, modification, or theft by malicious actors. A VPN (virtual private network) is a technology that protects data in transit by creating a secure tunnel between two endpoints and encrypting the data that passes through it.

References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 4, page 145.

NEW QUESTION 118

Which of the following is the most likely to be included as an element of communication in a security awareness program?

- A. Reporting phishing attempts or other suspicious activities
- B. Detecting insider threats using anomalous behavior recognition
- C. Verifying information when modifying wire transfer data
- D. Performing social engineering as part of third-party penetration testing

Answer: A

Explanation:

A security awareness program is a set of activities and initiatives that aim to educate and inform the users and employees of an organization about the security policies, procedures, and best practices. A security awareness program can help to reduce the human factor in security risks, such as social engineering, phishing, malware, data breaches, and insider threats. A security awareness program should include various elements of communication, such as newsletters, posters, videos, webinars, quizzes, games, simulations, and feedback mechanisms, to deliver the security messages and reinforce the security culture. One of the most likely elements of communication to be included in a security awareness program is reporting phishing attempts or other suspicious activities, as this can help to raise the awareness of the users and employees about the common types of cyberattacks and how to respond to them. Reporting phishing attempts or other suspicious activities can also help to alert the security team and enable them to take appropriate actions to prevent or mitigate the impact of the attacks. Therefore, this is the best answer among the given options.

The other options are not as likely to be included as elements of communication in a security awareness program, because they are either technical or operational tasks that are not directly related to the security awareness of the users and employees. Detecting insider threats using anomalous behavior recognition is a technical task that involves using security tools or systems to monitor and analyze the activities and behaviors of the users and employees and identify any deviations or anomalies that may indicate malicious or unauthorized actions. This task is usually performed by the security team or the security operations center, and it does not require the communication or participation of the users and employees. Verifying information when modifying wire transfer data is an operational task that involves using verification methods, such as phone calls, emails, or digital signatures, to confirm the authenticity and accuracy of the information related to wire transfers, such as the account number, the amount, or the recipient. This task is usually performed by the financial or accounting department, and it does not involve the security awareness of the users and employees. Performing social engineering as part of third-party penetration testing is a technical task that involves using deception or manipulation techniques, such as phishing, vishing, or impersonation, to test the security posture and the vulnerability of the users and employees to social engineering attacks. This task is usually performed by external security professionals or consultants, and it does not require the communication or consent of the users and employees. Therefore, these options are not the best answer for this question. References = Security Awareness and Training –

CompTIA Security+ SY0-701: 5.2, video at 0:00; CompTIA Security+ SY0-701 Certification Study Guide, page 263.

NEW QUESTION 122

An administrator discovers that some files on a database server were recently encrypted. The administrator sees from the security logs that the data was last accessed by a domain user. Which of the following best describes the type of attack that occurred?

- A. Insider threat
- B. Social engineering
- C. Watering-hole
- D. Unauthorized attacker

Answer: A

Explanation:

An insider threat is a type of attack that originates from someone who has legitimate access to an organization's network, systems, or data. In this case, the domain user who encrypted the files on the database server is an example of an insider threat, as they abused their access privileges to cause harm to the organization. Insider threats can be motivated by various factors, such as financial gain, revenge, espionage, or sabotage. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 1: General Security Concepts, page 251. CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 1: General Security Concepts, page 252.

NEW QUESTION 127

A company's end users are reporting that they are unable to reach external websites. After reviewing the performance data for the DNS servers, the analyst discovers that the CPU, disk, and memory usage are minimal, but the network interface is flooded with inbound traffic. Network logs show only a small number of DNS queries sent to this server. Which of the following best describes what the security analyst is seeing?

- A. Concurrent session usage
- B. Secure DNS cryptographic downgrade
- C. On-path resource consumption
- D. Reflected denial of service

Answer: D

Explanation:

A reflected denial of service (RDoS) attack is a type of DDoS attack that uses spoofed source IP addresses to send requests to a third-party server, which then sends responses to the victim server. The attacker exploits the difference in size between the request and the response, which can amplify the amount of traffic sent to the victim server. The attacker also hides their identity by using the victim's IP address as the source. A RDoS attack can target DNS servers by sending forged DNS queries that generate large DNS responses. This can flood the network interface of the DNS server and prevent it from serving legitimate requests from end users. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 215-216 1

NEW QUESTION 132

Several employees received a fraudulent text message from someone claiming to be the Chief Executive Officer (CEO). The message stated: "I'm in an airport right now with no access to email. I need you to buy gift cards for employee recognition awards. Please send the gift cards to following email address."

Which of the following are the best responses to this situation? (Choose two).

- A. Cancel current employee recognition gift cards.
- B. Add a smishing exercise to the annual company training.
- C. Issue a general email warning to the company.
- D. Have the CEO change phone numbers.
- E. Conduct a forensic investigation on the CEO's phone.
- F. Implement mobile device management.

Answer: BC

Explanation:

This situation is an example of smishing, which is a type of phishing that uses text messages (SMS) to entice individuals into providing personal or sensitive information to cybercriminals. The best responses to this situation are to add a smishing exercise to the annual company training and to issue a general email warning to the company. A smishing exercise can help raise awareness and educate employees on how to recognize and avoid smishing attacks. An email warning can alert employees to the fraudulent text message and remind them to verify the identity and legitimacy of any requests for information or money. References = What Is Phishing | Cybersecurity | CompTIA, Phishing – SY0-601 CompTIA Security+ : 1.1 - Professor Messer IT Certification Training Courses

NEW QUESTION 135

A systems administrator set up a perimeter firewall but continues to notice suspicious connections between internal endpoints. Which of the following should be set up in order to mitigate the threat posed by the suspicious activity?

- A. Host-based firewall
- B. Web application firewall
- C. Access control list
- D. Application allow list

Answer: A

Explanation:

A host-based firewall is a software application that runs on an individual endpoint and filters the incoming and outgoing network traffic based on a set of rules. A host-based firewall can help to mitigate the threat posed by suspicious connections between internal endpoints by blocking or allowing the traffic based on the source, destination, port, protocol, or application. A host-based firewall is different from a web application firewall, which is a type of firewall that protects web applications from common web-based attacks, such as SQL injection, cross-site scripting, and session hijacking. A host-based firewall is also different from an access control list, which is a list of rules that control the access to network resources, such as files, folders, printers, or routers. A host-based firewall is also different from an application allow list, which is a list of applications that are authorized to run on an endpoint, preventing unauthorized or malicious applications from executing. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 254

NEW QUESTION 136

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your SY0-701 Exam with Our Prep Materials Via below:

<https://www.certleader.com/SY0-701-dumps.html>